Firewall Anomaly Management: A survey

Abstract

Firewall secures a private network from intrusions from other networks. The firewall has ACLs (Access Control List) that contain rules used to allow or deny incoming traffic. These rules form the security policy of the firewall. The large size and complexity of modern networks result in large and complex firewall policies. Designing policies for a network of firewalls is a difficult task as a number of cases have to be taken into consideration for access control. Also, a network administrator may want to update the policies in order to replace them with new ones. The process of updating firewall policies is difficult and error prone. In this paper, we provide a structured and comprehensive overview of various techniques in regards to firewall anomaly
Firewall Anomaly Management: A survey

detection. We briefly describe and compare various known algorithms and tools used to detect and/or resolve the firewall anomalies.

References

  - Chi-Shih Chao, "A flexible and feasible anomaly diagnosis system for Internet firewall rules," 13th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2011
  - S. R. Pedditi, "An initial design of firewall information exchange protocol (FIEP)," MS Degree Project Report, Department of Computer Science, California State University, Sacramento, May 2012.
- Juniper Netscreen Series Security Systems, Juniper Networks Inc., Dec 2011
- Check Point Threat Prevention Appliances, Check Point Software Technologies, Ltd., 2012.

Index Terms

Computer Science Security

Keywords

firewalls ACL rules anomaly Firewall Policy Policy conflicts